BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DIEGO DIAS DOS SANTOS MARTINS

USO DE SISTEMA DE INFORMAÇÃO GEOGRÁFICA PARA LOCALIZAR CIBERTERRORISTAS; E ESTUDO APLICADO À SEGURANÇA OFENSIVA EM REDES CIBERNÉTICAS MUNDIAIS.

Niterói, RJ
2017

DIEGO DIAS DOS SANTOS MARTINS

USO DE SISTEMA DE INFORMAÇÃO GEOGRÁFICA PARA LOCALIZAR CIBERTERRORISTAS; E ESTUDO APLICADO À SEGURANÇA OFENSIVA EM REDES CIBERNÉTICAS MUNDIAIS.

Pré-Projeto de Conclusão de Curso apresentado ao Centro Universitário La Salle do Rio De Janeiro, como parte dos requisitos necessários à obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Alex Vanderlei Salgado

Coorientador: Prof. Dr.ª Márcia de Freitas

Niterói, RJ
Fevereiro de 2017

CENTRO UNIVERSITÁRIO LA SALLE DO RIO DE JANEIRO

CURSO DE SISTEMAS DE INFORMAÇÃO

Pré-projeto de conclusão de Curso apresentado ao Centro Universitário La Salle, em cumprimento parcial das exigências para obtenção do grau em Bacharel em Sistemas de Informação.

Aluno: Diego Dias dos Santos Martins

Título do Projeto: Uso de Sistema de Informação Geográfica para localizar ciberterroristas; e estudo aplicado à segurança ofensiva em redes cibernéticas mundiais.

Projeto aprovado em: _____/______/______

BANCA EXAMINADORA

____

Prof. Dr. Alex Vanderlei Salgado
Orientador

____

Prof. Dr.ª Márcia de Freitas Siqueira Sadok Menna Barreto
Coorientador

OBSERVAÇÕES:

____

____

____

____

SUMÁRIO

1 INTRODUÇÃO

Após os múltiplos atentados terroristas de 11 de setembro de 2001, nos EUA, logo se levantou a discussão sobre o ciberterrorismo como forma proeminente de segurança e terrorismo, uma vez que, o ciberterrorismo surge como oportunidade ao Estado Islâmico de causar danos em proporções ainda não vivenciadas.

O terrorismo cibernético é uma ameaça real devido ao rápido desenvolvimento tecnológico, onde os alvos potenciais são os sistemas que controlam as defesas e infraestruturas críticas das nações. O rápido crescimento dos usuários, bem como a dependência da Internet aumentaram drasticamente os riscos de segurança, ao menos que haja medidas de segurança adequadas para ajudar na prevenção, danos severos ou outras consequências sociais, ideológicas, religiosas e políticas poderão ser causados através do acesso de redes e sistema de informação em locais mais remotos do planeta.

Outra questão relevante, diz respeito à disposição em fazer parte de um grupo de ciberterroristas. Incialmente é um dos métodos mais baratos de terrorismo, pois necessita na maioria das vezes apenas de um computador pessoal e uma conexão on-line. Requer um número reduzido de pessoas. A dificuldade em rastrear a identidade real dos invasores facilita o anonimato e a quantidade de objetos-alvos é bastante variável.

Estudos demostram que as infraestruturas críticas, como as redes de energia elétrica e os serviços essenciais, são vulneráveis a ataques ciberterroristas porque os sistemas de informação que os executam são altamente complexos, tornando-os eficazes para ataques devido à impossibilidade de eliminar todas as fraquezas.

Desta forma é necessário que instituições governamentais de todo o mundo, se unam e tentem harmonizar as ações que constituem atividades criminosas no domínio cibernético para capacitar as agências de inteligência com tecnologia de segurança com intenção de investigar tais atividades e impedir tais ataques antes que causem consequências potencialmente danosas a sociedade global.

2 OBJETIVOS

2.1 Objetivo Geral

É dentro deste contexto, que o presente estudo tem como objetivo:

Elaborar um sistema de geolocalização capaz de detectar endereços de protocolos atribuídos a ciberterroristas pertencentes ao grupo jihadista Estado Islâmico (EI).

2.2 Objetivos Específicos

A fim de fomentar a proteção da informação:

1) Mostrar a importância da segurança e a defesa cibernética.

2) Ampliar a percepção dos riscos associados a novas ferramentas e meios de violação desenvolvidos por ciberterroristas para interceptarem os dados;

3) Garantir a estabilidade e integridade dos sistemas e;

4) Resguardar e preservar a confidencialidade das informações.

3 JUSTIFICATIVA

Nos dias atuais devido aos avanços tecnológicos e a globalização, cada vez mais a internet tem sido utilizada como meio para solucionar tarefas cotidianas. Um indivíduo pode acessar suas informações em qualquer parte, seja a mais remota do mundo. Assim, constantemente, dados como senhas de e-mails, contas bancárias, número de cartão previdenciário e crédito, estão trafegando pela rede entre um computador e outro.

Muitos são os dispositivos utilizados, como a exemplo os *firewalls*, antivírus e *antispyware* para tornarem a navegação digital mais segura, porém, infelizmente, os ciberterroristas também se adaptaram aos avanços da tecnologia e, assim, pessoas, organizações públicas e privadas estão se tornando, habitualmente, vítimas de violações cometidas através da Internet.

Em seu livro "*Terrorism, Crime, and Public Policy"* (2009), Brian Forst, expõe que grande parte dos ataques ciberterroristas tem como alvos estados políticos e instituições públicas, com ideologias políticas-religiosas, motivados a desestabilizar a ordem política, econômica e social.

Durante a apresentação do relatório anual de 2016, pela Organização do Tratado do Atlântico Norte (OTAN), o secretário-geral Jens Stoltenberg afirma que a instituição apresentou um aumento de 60% em relação a 2015, no número de ataques cibernéticos (EL PAÍS; 2017).

Apesar do Brasil não haver histórico de ataques terroristas, com a realização de grandes

eventos como a Jornada Mundial da Juventude em 2013, com a presença de Sua Santidade o Papa Francisco, a Copa das Confederações FIFA de 2014 e as Olimpíadas em 2016, o país tornou-se grande alvo de terrorismo, principalmente na esfera cibernética. Calcula-se que os Jogos Olímpicos de Londres, em 2012, tenham sofrido pelo menos 97 incidentes graves de segurança, envolvendo, principalmente, ataques de negação de serviço (DDoS). Diante disso, será preciso analisar a segurança em ciberespaços, pois estes são vitais para o recrutamento de combatentes do EI, bem como, para proteger principalmente os sistemas de controle de infraestrutura crítica, como a exemplo a rede de distribuição de energia e aeroportos, com o propósito de de evitar danos ou interrupções sérias, levando risco à sociedade (ALCÂNTARA, 2015; DATASUS; 2016).

4 HIPÓTESE

Há necessidade de assegurar a confiabilidade, a integridade das informações e a disponibilidade da comunicação, intensificando a identificação de vulnerabilidades nas estruturas de segurança da informação, a fim de aperfeiçoar a infraestrutura de proteção e minimizar os danos causados pelo grupo terrorista Estado Islâmico.

5 REFERENCIAL TEÓRICO

5.1 Atuação da perícia forense computacional.

Os ataques cibernéticos podem envolver uma quantidade muito ampla de métodos, que requerem procedimentos diferentes para melhorar a segurança computacional. Haja vista a eliminação de fronteiras oferecida pela Internet, sérias dificuldades acabaram-se desenvolvendo para combater esses tipos de delitos, tornando-se mais fácil sua prática e ocorrência onde vítimas e criminosos podem estar em países distintos e também distantes (FRANCO, 2016).

Neste contexto, surge a necessidade de uma área especializada com amplo conhecimento em computação, a segurança da informação, o direito digital e outras áreas afins, com capacidade suficiente para investigar quem, como e quando um crime cibernético foi praticado, assim surge a perícia forense computacional (FRANCO, 2016).

De acordo com o dicionário Aurélio de Língua Portuguesa, a palavra forense significa "*que se refere a foro judicial*" e a palavra perícia significa "*sabedoria, prática, experiência, habilidade em alguma ciência ou arte*". Desta maneira, a perícia forense computacional é a união entre conhecimentos da área da informática e da área jurídica, que por meio de métodos técnico-científicos, tem como objetivo coletar evidências digitais, analisar dados e apresentar provas perante um ambiente jurídico, visando sempre proteger usuários e recursos da

exploração, invasão de privacidade na forma digital e/ou qualquer outro crime (DE SOUZA; 2015; SOUZA; 2016).

Para a execução da perícia forense, Kent et. Al (2006) sugere uma sequência de procedimentos forense, que podem ser ajustados com o decorrer da perícia. A sequência é formada por quatro etapas (Figura 1):
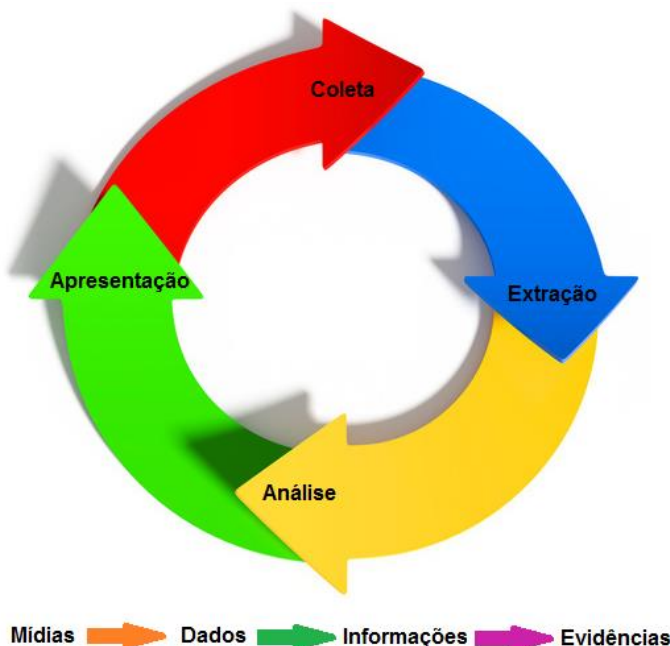
Figura 1: Etapas do processo forense
Fonte: Adaptado de KENT; et al. (2006).

- **Coleta**: é executada a identificação de elementos que provavelmente contenham evidências digitais ou que possuam alguma relação com o incidente que está sendo investigado;
- **Extração**: identificar, recuperar e extrair as informações relevantes a partir dos dados coletados utilizando ferramentas e técnicas forenses que sejam pertinentes à investigação;
- **Análise**: analisar os dados/informações do exame para elaborar respostas úteis para as questões apresentadas nas fases anteriores.
- **Apresentação**: tem como finalidade documentar as evidências digitais encontradas e apresentá-las às autoridades competentes. O laudo técnico pericial deve ser conciso, de fácil leitura, descrevendo de forma objetiva e clara os métodos, ferramentas e exames realizados durante o processo forense.

5.2 Espaço cibernético para práticas ilegais.

A sociedade moderna é marcada por um cenário em transformação pelo uso de alta tecnologia, introduzindo uma nova dimensão as formas de comunicação. A internet é uma realidade global que significa um grande marco para as comunicações. Manuel Castells (2003) afirma que a Internet constitui a base material e tecnológica da sociedade em rede, não sendo simplesmente uma tecnologia, mas um meio de comunicação que permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido, em escala global, sem fronteiras para restringir sua utilização.

O espaço físico e virtual passa a conviver com a complexidade da configuração cibernética. Neste sentido, surge o conceito de espaço cibernético, novo espaço onde ocorrem as relações humanas de grande importante, nas esferas políticas, econômicas, científicas e sociais. O espaço cibernético é "*a instauração de uma rede de todas as memórias informatizadas e de todos os computadores*" (LÉVY, 2007).

Com o avanço da tecnologia computacional e a da instauração de uma rede com todas as memórias informatizadas é importante compreender a ética da informática relacionada à segurança. Algumas perguntas necessitam ser abordadas quanto às questões éticas globais, tais como: - Quais informações sobre o indivíduo podem ser reveladas a outras pessoas? - Quais informações individuais devem ser mantidas em bancos de dados, e quão seguras são os sistemas de computador? - Como lidar com a pirataria de dados nas redes de computadores? - Como garantir que as informações sejam salvaguardas e só possam ser acessadas por pessoas e organizações autorizadas? (GUNARTO, 2017).

Neste contexto, com o crescimento de ferramentas gratuitas que são utilizadas para formular ataques, as poucas leis de prevenção de crimes digitais e o crescente número de grupos organizados que exploram as deficiências de segurança, veem se apontando as oportunidades para o cibercrimes (ÂNGELO, 2002).

Entende-se por cibercrimes ou crime virtual qualquer ação que infringem as normas éticas uma vez que esses prejudicam a sociedade em geral, onde o computador seja o instrumento ou objeto do delito, ou então, qualquer delito ligado ao tratamento automático de dados (VAREJÃO, 2004).

Com a investigação dos cibercrimes, surgiu à necessidade de caracterizar um perfil dos grupos que cometem esses crimes, assim surgiu o personagem *"Hacker".* Segundo tradução do dicionário Michaelis o termo *Hacker*, quer dizer "*indivíduo que se dedica a entender o funcionamento interno de dispositivos, programas e redes de informática com o fim, entre*

outras coisas, de encontrar falhas em sua segurança ou conseguir um atalho inteligente que possa vir a resultar em um novo recurso ou ferramenta". Porém, como têm sido divulgados por muito tempo através das mídias mundiais, os hackers são denominados indivíduos que invadem os sistemas de segurança e quebram os códigos computacionais para fins ilegais como, por exemplo, fraudar sistema telefônico, copiar programa de computador ou material audiovisual, fonográfico etc., sem autorização do autor ou sem respeito aos direitos de autoria e cópia, para comercialização ou uso pessoal. Assim, os *Hackers* criaram a termo "*Cracker*", oriundo de *Criminal Hacker*, para nomear estes tipos de criminosos que em geral, são repudiados pelos membros das comunidades internacionais de software livre (AGUIAR, ET AL.; 2009).

Desta maneira, o vasto conhecimento aprofundado em tecnologia de sistemas entre hackers e os crackers geralmente são muito parecidos, porém, a principal diferença é a finalidade do uso deste conhecimento e as práticas resultantes. Enquanto os crackers são motivados por objetivos criminosos de obter vantagens de formas ilícitas, os hackers realizam atividades positivas, de desenvolvimento e aperfeiçoamento. Assim, por onde os Crackers percorrem os Hackers seguem seus passos para evitar que os problemas causem maiores danos.

Com a evolução da tecnologia, as ameaças cibernéticas podem ser executadas de diferentes formas, o que diferenciará o tipo de ataque dependerá do objeto-alvo e da motivação, sendo os tipos de ameaças agrupadas em (IDN; 2013):

- **Cibercrime**: Essencialmente de característica de benefício econômico próprio através de ações ilegais, como fraudes bancárias, roubo de número de cartão de crédito e transações financeiras.

- **Ciberespionagem**: O foco principal é obtenção de informações importantes, seja de organizações governamentais ou privadas, para obtenção de benefício próprio ou posterior venda.

- **Ciberterrorismo**: Busca-se um impacto social e político significativo pela destruição de infraestruturas críticas.

- **Ciberguerra**: Constitui conflitos entre diferentes nações e o ciberespaço é o ambiente de batalha.

5.3 Uso de Sistemas de Informações Geográficas.

Pretendendo localizar cada ponto da superfície do globo terrestre, fora criado um sistema de linhas imaginárias intitulado de Sistema de Coordenadas Geográficas. A coordenada geográfica de um ponto específico da superfície do planeta é resultante da interseção de um meridiano e um paralelo (RECESA, 2013).

Os Meridianos são linhas imaginárias que cortam a Terra no sentido Norte-Sul, ligando um polo ao outro. O meridiano central (Greenwich) divide a Terra em dois hemisférios e a sua gradação vai até 180º tanto para Leste (E) quanto para Oeste (W). Os paralelos são círculos da esfera cujo plano é perpendicular ao eixo dos polos. O equador é o paralelo que divide a Terra em dois hemisférios (Norte e Sul). A linha do Equador corresponde ao paralelo de origem (0º), seguindo a 90º em direção aos polos, indicando a posição no hemisfério Sul (S) ou no hemisfério Norte (N) (TERRAVIEW; 2011; RECESA; 2013).

Assim, as coordenadas geográficas que definem um ponto específico na Terra correspondem ao conjunto da latitudes e longitudes. Onde longitude é o valor angular do arco compreendido entre o meridiano de Greenwich (0º) e o lugar de referência que varia entre 0° a ±180° (W/E) e latitude é o valor angular do arco compreendido entre o equador e o lugar de referência que varia de 0° a ±90° (N/S) (MARQUES; 2017).

A partir da metade do século XX, por meio do uso da informática, possibilitou-se fazer análises criteriosas de projeção cartográfica combinando diferentes mapas e dados, uma vez que há uma variedade de modos de projetar sobre um plano os objetos geográficos que caracterizam a superfície terrestre, dando origem ao geoprocessamento (TERRAVIEW; 2011).

Segundo Câmara e Davis (2001) geoprocessamento denota a disciplina do conhecimento que utiliza técnicas matemáticas e computacionais para o tratamento da informação geográfica. Moreira, et. al. (2012), complementa que o geoprocessamento pode tratar dados de objetos ou fenômenos geograficamente identificados ou extrair informações desses objetos ou fenômenos, quando eles são observados por um sistema sensor.

Desta maneira o geoprocessamento tem sido amplamente empregado na Cartografia, Análise Ambiental, Transporte, Energia, Planejamento Urbano, Saúde e mais recentemente na Segurança Pública. Para cada uma dessas áreas é necessário um sistema específico. As ferramentas computacionais para executar o geoprocessamento são chamadas de Sistemas de Informação Geográfica (SIG ou (inglês) – *Geographic Information Systems*), que permite realizar análises complexas, ao integrar dados de diversas fontes e criar bancos de dados georreferenciados (NICOLAU; 2005).

Teixeira et al. (1995), define SIG como um conjunto de programas, equipamentos, metodologias, dados e pessoas (usuários), perfeitamente integrados, de forma a tornar possível a coleta, o armazenamento, o processamento e a análise de aplicação. O SIG visa propor maior facilidade, segurança e agilidade nas atividades humanas referentes ao monitoramento, planejamento e tomada de decisão relativas ao espaço geográfico.

Um SIG, possui a seguinte estrutura (CÂMARA; DAVIS; 2001):

- Interface com usuário;
- Entrada e integração de dados;
- Funções de processamento gráfico e de imagens;
- Visualização e plotagem; e
- Armazenamento e recuperação de dados (organizados sob a forma de um banco de dados geográficos).

Estes componentes fundamentais que configuram um SIG, devem funcionar em plena harmonia e integração para que o sistema funcione satisfatoriamente (Figura 2).

Figura 2: Componentes de um SIG.
Fonte: http://geoinfoproyecto.blogspot.com, 2012.

Os dados agora georreferenciados podem ser utilizados nas mais variadas aplicações, tornando-se uma poderosa ferramenta no auxílio à tomada de decisões, pesquisas, entre outros, como, por exemplo: aquelas que envolvem o uso da terra, seres humanos e a infraestrutura existente; aplicações ambientais, enfocando o meio ambiente e o uso de recursos naturais; aplicações de gerenciamento, de como alocar recursos para remediar problemas ou garantir a preservação de determinadas características; e de modo mais recente para análises criminais (NICOLAU, 2005).

Há uma crescente mudança dos crimes no século XXI, que se expandiu para os ciberespaços, dentre eles o terrorismo cibernético. O ciberespaço é uma ameaça real e no futuro, será pelo menos tão perigoso quanto o campo de batalha físico. Assim, as tecnologias

geoespaciais estão sendo adaptadas combinando tecnologias de vigilância, dados e SIG, bem como as práticas de monitoramento, identificação e captura com o objetivo de proteger as informações empresariais e governamentais contra os ataques de ciberterroristas (LATTIMER, 2013).

5.4 Estratégias de segurança ofensiva de redes cibernéticas.

O avanço das chamadas tecnologias de informação e comunicação (TICs) trouxeram grandes benefícios, no entanto, fizeram surgir um dos maiores desafios do novo século em termos de segurança, os ataques cibernéticos.

Segundo o Departamento de Segurança Interna dos Estados Unidos, a segurança cibernética inclui a vigilância aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e a respectiva informação neles contida, tendo em vista preservar a confidencialidade, integridade e disponibilidade, incluindo ainda ações para restabelecer a informação eletrônica e os sistemas de comunicações no caso de um ataque terrorista ou de um desastre natural (NIPP; 2009).

Com o acelerado ritmo de competitividade do mercado em lançar novos produtos tecnológicos, dentre *hardware* e *software*, sem que estejam completamente testados, gerando equipamentos com potenciais problemas de funcionamento assim, cria-se uma nova vulnerabilidade estrutural e funcional das redes e também dos sistemas que unificam as infraestruturas de informação (IDN, 2013).

Outro fator relevante, de grande preocupação refere-se à dependência do pleno funcionamento das redes de telecomunicações para a operação de infraestruturas críticas como as centrais de produção e distribuição de energia elétrica, os serviços de emergência, o sistema bancário e os próprios sistemas de comando e controle das Forças Armadas,

Diante do risco presente, a segurança e a proteção contínua das infraestruturas de informação têm de ser vista como um processo contínuo e sistêmico. Desta maneira, empresas e organizações voltadas para o desenvolvimento de tecnologias de informação, constituem um mecanismo destinado a desvendar vulnerabilidades que provoquem erros em seus produtos.

Em função da sensibilidade das informações é necessário estabelecer uma estratégia ofensiva, ou seja, uma abordagem proativa e hostil para proteger, sistemas, redes e indivíduos de ataques. A segurança convencional, por vezes referida como "segurança defensiva", centra-se em medidas conservadoras, tais como correção de software, encontrar e corrigir vulnerabilidades do sistema. Em contraste, as medidas de segurança ofensivas estão focadas na

busca dos invasores e em alguns casos tentar desativar, interromper ou pelo menos minimizar os impactos de suas operações.

Na era da informação, ao que diz respeito ao âmbito militar, o próprio ciberespaço é utilizado para conduzir todo o conjunto das operações, dando origem ao conceito de Operações no Ciberespaço, ou *Computer Network Operations* (CNO), cujo Departamento de Defesa dos Estados Unidos (DoD – *United States Department of Defense*) instrui que o CNO para explorar possíveis capacidades dos adversários deve ser composto de:

- ***Computer Network Defense (CND):*** Medidas defensivas para proteger e defender informações, computadores e redes de ataques de interrupção, negação, degradação ou destruição.
- ***Computer Network Exploitation (CNE):*** Técnica onde redes de computadores são utilizadas para infiltrar outras redes de computadores alvo para extrair e recolher dados de inteligência. Permite a exploração de computadores individuais e redes de computadores de uma organização ou país externo, a fim de recolher dados vulneráveis ou confidenciais, que normalmente são mantidos ocultos e protegidos do público em geral.
- ***Computer Network Attack (CNA):*** Operações para interromper, negar, degradar, ou destruir informações nas redes de comunicação de possíveis adversários ou em computadores, redes e sistemas próprios.

Diante da crescente habilidade em interromper e destruir os sistemas de informação e telecomunicações. A OTAN e a UE tem unido esforços junto aos EUA, diante das ameaças globais atribuídas aos ciberespaços (IDN, 2013).

6 PROCEDIMENTOS METODOLÓGICO

Para a realização deste trabalho propõem-se os seguintes passos descritos abaixo.

1) Escolha do tema:

De acordo com alguns estudos, os grupos terroristas extremistas veem fazendo uso das tecnologias de telecomunicação para recrutar, treinar, financiar, divulgar e realizar atos de violência pelo mundo. Reconhecer o perfil e a localização desta organização, tarefa sugerida por este projeto demonstra sua importância no contexto de Segurança Pública mundial.

2) Pesquisa de referências bibliográficas nacionais e internacionais sobre o assunto abordado:

Através de pesquisas à Internet em sites e repositores de publicações científicas de Universidades nacionais e internacionais pôde-se obter um conjunto significativo de

bibliografias e informações sobre o assunto abordado.

3) Etapas para o desempenho do software NetCriminals (Figura 3):

a. **Coleta**: A equipe de investigação forense computacional fará busca na Internet por pessoas, grupos e perfis que possuam características que possam associá-los de alguma forma a grupos terroristas. As evidências forenses que levem a indícios suspeitos, se dará pela investigação e coleta de dados dos suspeitos nos ambientes *surface web* (partes indexadas) e ambientes *deep weeb* (não-indexados) utilizando como ferramenta o buscador Google, com uso de navegadores convencionais como Chrome, Mozilla Firefox, Internet Explorer e o buscador Grams que utilizam as ferramentas intermediárias Tor ou Tor2web.

b. **Extração**: As informações geográficas dos suspeitos serão fornecidas pelo NetCriminals a partir da inserção de um IP ou de uma URL.

c. **Funcionamento do software**: O NetCriminals será construído em linguagem *Perl*, utilizando biblioteca do módulo *Comprehensive Perl Archive Network* (CPAN) que possui ferramentas que irão garantir a qualidade do software. O NetCriminals obterá dados de provedores de internet e endereços de site através da integração com o sistema API-IP. Este sistema irá consultar o mecanismo de layout Gecko que foi desenhado para suportar os padrões abertos da Internet como HTML, Javascript, DOM, XML, dentre outros. Com o objetivo em obter dados, o Gecko se interligará ao GetKong que também é um intermediador entre sistemas e de bancos de dados geográficos. Ao final esses dados retornarão sistema API-IP e para o NetCriminals a fim de gerar informações.

d. **Análise**: Como posse dos dados obtidos pelo NetCriminals será realizada uma análise quanto a conduta comportamental dos suspeitos, para determinar se estes se enquadram em um perfil de ciberterroristas.

e. **Apresentação**: Serão demonstrados dados em forma de mapas para facilitar o entendimento da localização dos suspeitos. Estes mapas serão disponibilizados através dos serviços do sistema Google Earth que ilustra o mapeamento da informação geográfica.

.
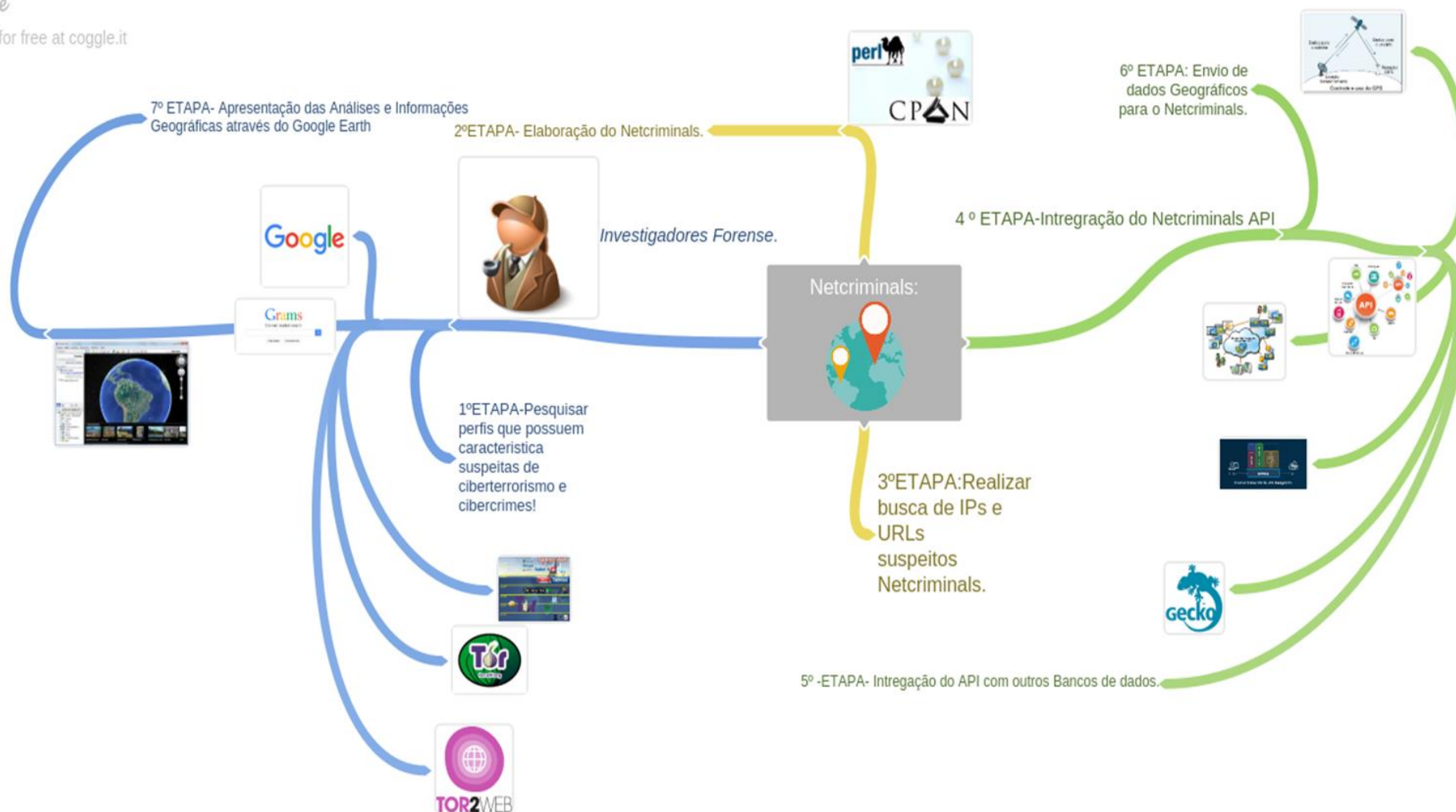
Figura 3: Mapa mental do funcionamento do sistema NetCriminals.

7 RESULTADOS ESPERADOS

Os resultados obtidos neste projeto poderão subsidiar a elaboração de políticas de apoio os planos de segurança pública, a partir da união de vários serviços de inteligências em diferentes países, que atuarão contra ataques terroristas e crimes cibernéticos. Além disso, este projeto pelo uso do Sistema de Informação Geográfica irá permitir a localização de servidores, inclusive proporcionará o desenvolvimento de técnicas de testes de invasão para identificar falhas nos sistemas dos ciberterroristas e de outros indivíduos que desejam realizar crimes cibernéticos. O projeto demonstrará os perigos que podem ocorrer na Internet através da tentativa legal e autorizada de localizar e explorar sistemas de computadores de forma bem-sucedida com o intuito de tornar esses sistemas mais seguros, a fim de solucionar essas falhas e tornar este ambiente seguro para as pessoas e para as diferentes organizações.

8 CRONOGRAMA

2017	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
1	X	X	X	X	X	X	X	X	X	X	X	X
2			X									
3				X	X	X	X	X	X	X	X	
4							X	X	X			
5										X	X	
6												X

1. Revisão de bibliografia
2. Apresentação do Pré-projeto
3. Coleta e organização dos dados
4. Análise dos dados e construção do sistema
5. Redação do Projeto Final
6. Apresentação do Projeto Final

REFERÊNCIAS

AGUIAR, V.M. (Org). **Software livre, cultura hacker e o ecossistema da colaboração**. - São Paulo: Momento Editorial, 2009.

ALCÂNTARA, B. T. **Brasil e Ciberterrorismo: desafios para o Rio 2016**. *International Conference on Forensic Computer Science* (ICOFCS). 2015, Brasília. Disponível em: <http://www.icofcs.org/2015/ICoFCS-2015-011.pdf> Acesso em: 18 mar. 2017.

ÂNGELO, F. K. Brasil lidera ranking mundial de hackers e crimes virtuais. **Folha de São Paulo**, 2002 http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml> Acesso em 13 mar. 2017.

CÂMARA, G; DAVIS, C. Por que geoprocessamento? In: CÂMARA, G; et al. (Org.) **Introdução à Ciência da Geoinformação**. São José dos Campos: INPE, 2001. p. 1-5. Disponível em: <http://www.dpi.inpe.br/gilberto/livro/introd/cap1-introducao.pdf> Acesso em: 13 mar. 2017.

CASTELLS, M. A galáxia da Internet. Rio de Janeiro: Jorge Zahar, 2003.

DA SILVA ROMERO, C. W.; DE MACEDO, F. L.; SILVA, H. R. Avaliação Ambiental da Bacia Hidrográfica Córrego da Onça Guaraçai–SP. **Periódico Eletrônico Fórum Ambiental da Alta Paulista**, v. 8, n. 2, 2012.

DATASUS. Departamento de Informática do SUS. **Rio 2016: Tendência é de aumento de ciberataques a empresas e executivos**. 2016. Disponível em: <http://datasus.saude.gov.br/seguranca-da-informacao/noticias-seguranca-da-informacao/1016-rio-2016-tendencia-e-de-aumento-de-ciberataques-a-empresas-e-executivos> Acesso em: 18 mar. 2017.

DE SOUZA, P. F. C. **Perícia Forense Computacional**: procedimentos, ferramentas disponíveis e estudo de caso. Santa Maria: UFSM, 2015. 74p. (Trabalho de Conclusão de Curso) Curso Superior de Tecnologia em Redes de Computadores da Universidade Federal de Santa Maria, Santa Maria, 2015.

El PAÍS. ***Los ciberataques a la OTAN crecieron un 60% en 2016***. Disponível em: <http://internacional.elpais.com/internacional/2017/03/13/actualidad/1489425600_231212.html> Acesso em: 18 mar. 2017

FORST, B. ***Terrorism, Crime and Public Policy***, Cambridge University Press, 2009.

FRANCO, D. P. A Atuação do Perito Forense Computacional na Investigação de Crimes Cibernéticos. **Revista Cryotoid.** 2016. Disponível em: <https://cryptoid.com.br/banco-de-noticias/atuacao-do-perito-forense-computacional-na-investigacao-de-crimes-ciberneticos/> Acesso em: 13 mar. 2017.

GUNARTO, H. ***Ethical Issues in Cyberspace and IT Society***. Ritsumeikan Asia Pacific University. 2017. Disponível em: <http://www.apu.ac.jp/~gunarto/it1.pdf> Acesso em 13 mar. 2017.

IDN. Instituto da Defesa Nacional. **Estratégia da Informação e Segurança no Ciberespaço**. Lisboa: 2013. Disponível em: <http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf> Acesso em 14 mar. 2017.

KENT, K. et al. **Guide to integrating forensic techniques into incident response: recomendations of the National Institute of Standards and Technology. Special publication. Gaithersburg**: NIST, 2006.

LATTIMER, C. ***The Future of Geospatial Technologies in Securing Cyberspace.*** E-International Relations Students, 2013. Disponível em: <http://www.e-ir.info/2013/08/03/the-future-of-geospatial-technologies-in-securing-cyberspace/> Acesso em: 13 mar. 2017.

LÉVY, P. **Cibercultura**. Lisboa: Instituto Piaget, 1997.

MARQUES, R. **Fundamentos de Cartografia**: a Rede Geográfica. Departamento de Geociências. Universidade Federal da Paraíba, 2017. Disponível em: <http://www.geociencias.ufpb.br/leppan/disciplinas/lic/aula2.pdf> Acesso em: 13 mar. 2017.

MOWBRAY, T. J. ***Cybersecurity****: Managing Systems, Conducting Testing, and Investigating Intrusions*. John Wiley & Sons. Indianapolis: 2008. Disponível em: <https://sqnetworks.com/uploads/Zachman-Framework-Cybersecurity.pdf> Acesso em 14 mar. 2017.

NICOLAU, L. A. **Sistema de informação geográfico-gerencial aplicado à gestão da qualidade na Segurança Pública.** Minas Gerais: UFLA, 2005. 80p. (Monografia) Departamento de Ciência da Computação da Universidade Federal de Lavras, Lavras, 2005.

NIPP. ***National Infrastructure Protection Plan****: Partnering to enhance protection and resiliency*, DHS, 2009. Disponível em: <https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf> Acesso em 14 mar. 2017.

RECESA. Rede de Capacitação e Extensão Tecnológica em Saneamento Ambiental. **Princípios básicos de geoprocessamento para seu uso em saneamento**. 2013. Disponível em: <http://nucase.desa.ufmg.br/wp-content/uploads/2013/07/principios-basicos-de-geoprocessamento.pdf> Acesso em: 13 mar. 2017.

SOUZA, A. G. Etapas do processo de computação forense: uma revisão. **Rev. Acta de Ciência e Saúde**. n. 5, v. 02, 99- 111p. 2016. Disponível em: <http://www2.ls.edu.br/actacs/index.php/ACTA/article/view/138> Acesso em: 13 mar. 2017.

TEIXEIRA, A.; et al. Qual a melhor definição de SIG, **Revista Fator GIS**, nº 11 Ano 3, Sagres Editora, Curitiba, 1995.

TERRAVIEW. **Conceitos Cartográficos**. 2011. Disponível em: <http://www.dpi.inpe.br/terraview/docs/pdf/ProjecaoCartografica.pdf> Acesso em: 13 mar. 2017.

VAREJÃO, F. **Ética e Crimes Virtuais**. UFES, 2004. Disponível em: <http://www.inf.ufes.br/~fvarejao/cs/eticapeique.htm> Acesso em 13 mar. 2017.